**Политика Информационной безопасности ООО «Богатенький нефтяник»**

**1. Общие положения**

1.1. Достижение стратегический целей ООО «Богатенький нефтяник» связано с управление информацией, являющейся важный информационным ресурсом. Информационная безопасность – это один из главных факторов успешной и стабильной работы компании. Обеспечение ИБ сотрудников и клиентов компании является одной из первостепенных задач.

1.2. Политика является документом, доступным любому сотруднику компании «Богатенький нефтяник» и пользователю её ресурсов.

**2. Основные цели и задачи**

2.1. Политика направлена на достижение следующих основных целей:  
1) Защита информации от всевозможных видов угроз;  
2) Развитие и обеспечение компании в области ИБ;  
3) Предотвращение утечки информации;

2.2. Основными задачами политики являются:  
1) Защита информационных ресурсов, содержащих коммерческую тайну, персональные данные физических лиц, а также любую другую информацию ценную для компании.  
2) Защита сотрудников компании, являющихся разработчиками, которые обеспечивают функционирование компании в информационной сфере.  
3) Защита информационной инфраструктуры, включающую в себя системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения  
4) Информирование, обучение, контроль знаний работников компании по вопросам ИБ  
5) Законности - соблюдение законодательства по защите информации и законных интересов всех участников информационного обмена;  
6) Совершенствовании - совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;7) Соответствие стандартам - система информационной безопасности соответствует международным стандартам в данной области;

**3. Организационное обеспечение информационной безопасности**

3.1. Система распределения обязанностей между отдельными работниками может в значительной мере способствовать повышению общего уровня информационной безопасности. Этого можно достичь следующими методами:   
3.1.1. Минимизация данных, доступных работникам. Каждый работник должен знать только те детали процедур обработки данных, которые необходимы ему для выполнения своих обязанностей. Организация технологического процесса сбора и обработки информации и планирование помещений должны по мере возможности исключать или сводить к минимуму контакты персонала в процессе выполнения работ. Каждый работник должен знать все о своей работе и связанных с нею ограничениях, а также четко представлять последствия нарушения этих ограничений;   
3.1.2. Разделение полномочий и дублирование контроля. В системах с высокими требованиями по обеспечению сохранности данных ответственная работа или процедура (например, изменение статуса электронного документа) выполняется после подтверждения ее необходимости двумя работниками. Временные или вновь принятые работники, а также работники, проходящие обучение, стажировку, практику не должны самостоятельно выполнять ответственные задания.  
  
3.2. В работе с работником компании основными организационными мерами в плане достижения информационной безопасности являются:   
3.2.1. Заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности и сохранность конфиденциальной информации;   
3.2.2. Проведение первоначального инструктажа, периодического обучения и повышения квалификации работников компании в области информационной безопасности.

**4. Требования и рекомендации**

4.1. Ответственность за информационные активы.  
В отношении всех собственных информационных активов Компании, активов, находящихся под контролем Компании, а также активов, используемых для получения доступа к инфраструктуре Компании, должна быть определена ответственность соответствующего сотрудника Компании. Эта ответственность указывается в трудовых договорах и в должностных инструкциях сотрудников Компании.

4.2. Контроль доступа к информационным системам

**5. Заключительные положения**

5.1. Требования настоящей политики могут развиваться другими внутренними документами компании, которые дополняют и уточняют ее.  
  
5.2. Ежегодно пересматриваются основные принципы, направления и требования по защите информации в компании. Пересмотр политики осуществляется в соответствии с изменениями, влияющими на первоначальную оценку риска, путем выявления существенных инцидентов нарушения информационной безопасности, появления новых уязвимостей или изменения организационной, или технологической инфраструктуры компании.  
  
5.3. Ответственным за внесение изменений в настоящую политику является руководитель ответственного подразделения.